

Proyecto de Decreto del Consell, por el que se establece la política de la seguridad de la información de la Administración de la Generalitat.

ÍNDICE

PREÁMBULO	2
CAPÍTULO I	5
DISPOSICIONES GENERALES.....	5
Artículo 1. Objeto.	5
Artículo 2. Ámbito Subjetivo de aplicación.	5
Artículo 3. Definiciones.....	5
CAPÍTULO II	5
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	5
Artículo 4. Principios rectores y requisitos mínimos de seguridad.	5
Artículo 5. Misión de la Administración de la Generalitat.....	6
Artículo 6. Marco regulatorio.	6
Artículo 7. Desarrollo normativo.	6
Artículo 8. Riesgos derivados con el tratamiento de datos personales.....	7
CAPÍTULO III	7
ORGANIZACIÓN DE LA SEGURIDAD	7
Artículo 9. Estructura, niveles de responsabilidad y roles de seguridad.....	7
Artículo 10. Los Responsables de la Información.....	7
Artículo 11. Los Responsables del Servicio.....	8
Artículo 12. El Responsable de Seguridad.	8
Artículo 13. Responsable del Sistema.....	9
Artículo 14. Administrador de la Seguridad del Sistema.....	9
DISPOSICIONES ADICIONALES	10
Primera. Incidencia presupuestaria.....	10
Segunda. Inclusión al ámbito subjetivo de esta PSI.....	10
Tercera. Coordinación global de la ciberseguridad en la Administración de la Generalitat.....	10

Cuarta. Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV).	10
DISPOSICIÓN DEROGATORIA	11
Única. Disposiciones que se derogan.	11
DISPOSICIONES FINALES.....	11
Primera. Ampliación de funciones de seguridad corporativa a la CITEC.....	11
Segunda. Organización de la seguridad en la Administración Sanitaria.....	12
Tercera. Organización de la seguridad en la Administración Educativa.	12
Cuarta. Organización de la seguridad en la Administración de Justicia.	13
Quinta. Desarrollo.	13
Sexta. Entrada en vigor.	13

PREÁMBULO

El Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat y el Decreto 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat, requieren una profunda revisión debido a las numerosas modificaciones tanto de marco normativo europeo como el español, por lo que, de conformidad con las directrices establecidas en el artículo 3.4 del Decreto 24/2009, de 13 de febrero, del Consell, sobre la forma, la estructura y el procedimiento de elaboración de los proyectos normativos de la Generalitat, que establece como criterio que las disposiciones modificativas sean utilizadas con carácter restrictivo, debiendo primar la aprobación de una nueva disposición sobre el mantenimiento de la norma originaria y sus posteriores modificaciones, se opta por la aprobación de un nuevo Decreto que aglutine tanto la política como la organización de la seguridad en toda la Administración de la Generalitat. Es aplicable a la Presidencia, a las consellerías de la Administración de la Generalitat y a los entes del sector público institucional de la Generalitat que determinen adherirse; facultando a la consellería con competencias en sanidad, a la consellería con competencias en educación, a la consellería con competencias en justicia, para que desarrollen las disposiciones necesarias para establecer la organización de la seguridad de la información en determinados ámbitos de su competencia.

Básicamente, en este decreto se establece una política de seguridad acorde con la nueva realidad respecto a la progresiva transformación digital en nuestra sociedad, el nuevo escenario de ciberseguridad, el avance de las tecnologías de la información y la evolución de las amenazas; incluyendo la designación de una serie de responsables en materia de seguridad de la información, asignándoles funciones y responsabilidades, regulando la organización e implantación del proceso de seguridad.

Los importantes cambios normativos producidos desde su entrada en vigor, provocan una necesaria adaptación de la organización de la seguridad: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; y especialmente la aprobación reciente del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Además, el Estado ha aprobado toda una serie de Instrucciones Técnicas de Seguridad, que hay que tener en consideración: la Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad; la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información; la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad; y la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

También a nivel autonómico se han producido cambios relevantes: la derogación de la Ley 3/2010, de 5 de mayo, de administración electrónica de la Comunitat Valenciana; la modificación de la Ley 3/2005, de 15 de junio, de la Generalitat, de Archivos; el Decreto 20/2020, de 14 de febrero, del Consell, de modificación del Decreto 112/2008, por el cual se crea la Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana; así como la creación y asignación de funciones del Delegado o la Delegada de Protección de Datos de la Administración de la Generalitat con la ORDEN 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática, por la que se desarrolla el Decreto 179/2020, de 30 de octubre, del Consell, por el cual se aprueba el Reglamento orgánico y funcional de la Conselleria de Participación, Transparencia, Cooperación y Calidad Democrática.

El presente Decreto se ha configurado siguiendo las directrices de la *Guía de Seguridad de las TIC CCN-STIC 801*, editada por el Centro Criptológico Nacional, sobre responsabilidades y funciones en el Esquema Nacional de Seguridad y definen exclusivamente los roles de seguridad correspondientes al Esquema Nacional de Seguridad.

La estructura organizativa que define el decreto simplifica el modelo actualmente vigente y descentraliza en gran medida las responsabilidades de seguridad de la información en las consellerías y entidades.

En el nivel de gobierno, acerca las responsabilidades de la información y del servicio a los órganos directivos competentes en el contenido y funcionalidad de cada sistema de información. Es habitual que coincidan en la misma persona las responsabilidades de la Información y del Servicio; pero tiene sentido la diferenciación cuando la prestación del servicio maneja información de diferentes procedencias, así como cuando la prestación del servicio no depende del órgano que es Responsable de la Información.

En el nivel de supervisión, concentra la responsabilidad de la seguridad de la información en el órgano de carácter directivo que tiene atribuidas las competencias sobre los servicios generales de cada entidad, como agente clave para coordinar la seguridad en todos los aspectos: física, jurídica, recursos humanos, administrativa, archivo, comunicación, información, privacidad y tecnología.

En el nivel operativo, asigna la responsabilidad del sistema al órgano directivo competente en materia de

tecnologías de la información y designa directamente a los administradores de seguridad del sistema, vinculando la administración de la seguridad como una parte intrínseca de la administración de los sistemas.

Respecto al Comité de Seguridad de la Información, se suprime como tal, integrando las funciones principales de seguridad corporativa a la ya existente Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana (CITEC).

En cuanto a la coordinación global de la ciberseguridad en toda la Administración de la Generalitat, conforme al Acuerdo del Consell sobre esta materia, se atribuye la coordinación global en ciberseguridad para toda la Administración de la Generalitat a la unidad administrativa con competencias en ciberseguridad del órgano directivo con competencias en materia de tecnologías de la información.

La Política de Seguridad de la Información Judicial Electrónica (PSIJE) tiene como finalidad definir la utilización de medios electrónicos en el ámbito de la Administración de Justicia, así como el establecimiento del marco organizativo y tecnológico de la misma; se aplica a todos los sistemas de información y comunicación utilizados para la Administración de Justicia por todos los órganos, departamentos y unidades del Consejo General del Poder Judicial (CGPJ), de la Fiscalía General del Estado, del Ministerio de Justicia y de las Comunidades Autónomas (CCAA) que tienen transferidas las competencias en esta materia, así como en los organismos públicos que dependan de los mismos. En la PSIJE se determina para los sistemas auxiliares de la Administración de Justicia, qué funciones asumirán las administraciones con competencia en materia de justicia; con este fin, puesto que la Comunitat Valenciana tiene asumidas las competencias en materia de justicia, el decreto faculta a la persona titular de la Conselleria con competencias en justicia para que desarrolle las disposiciones necesarias para establecer la organización de la seguridad de la información para las funciones que son determinadas para las CCAA en la PSIJE.

En cuanto a la coordinación entre las responsabilidades de protección de datos y de seguridad de la información, el responsable de seguridad integrará los resultados de los análisis de riesgos en materia de protección de datos, y en su caso de las evaluaciones de impacto, con las declaraciones de aplicabilidad, de forma que en un único plan de seguridad para cada sistema de información se contemplen todas las medidas técnicas y organizativas que deban implantarse.

La aprobación de este decreto estaba prevista en el Plan Normativo de la Administración de la Generalitat 2021.

En la tramitación de esta norma se han respetado los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas. El respeto al principio de necesidad ha quedado justificado en el presente preámbulo por los cambios normativos producidos en el ámbito de la normativa europea y nacional. La norma establece la organización de la política de la seguridad de la información conforme a los principios de eficacia y proporcionalidad, por ello establece una estructura orgánica con base en los órganos y unidades administrativas existentes en la administración del Consell y su sector público y las funciones que desempeñan. Asimismo, se dicta en coherencia con lo dispuesto en el resto del ordenamiento jurídico nacional y de la Unión Europea, manteniendo un marco normativo integrado y claro en aras al respeto del

principio de seguridad jurídica. Por último, con fundamento en el principio de eficiencia y la política en materia de gasto, el presente decreto no implica aumento del gasto.

En virtud de lo dispuesto en la disposición final segunda sobre desarrollo normativo del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, conforme a lo dispuesto en los artículos 31 y 33 de la Ley 5/1983, de 30 de diciembre, del Consell, previo el cumplimiento de los trámites preceptivos establecidos en el artículo 43 de la misma ley, a propuesta del Conseller de Hacienda y Modelo Económico, y previa deliberación del Consell, en la reunión del día ---- de --- de ----,

DECRETO

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto.

El objeto del presente Decreto es establecer la política de la seguridad de la información (en adelante, PSI) determinando su estructura y detallando las atribuciones para cada uno de los roles que la conforman.

Artículo 2. Ámbito Subjetivo de aplicación.

La PSI regulada en el presente decreto es aplicable a la Administración de la Generalitat.

Artículo 3. Definiciones.

A los efectos previstos en este decreto las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el glosario de términos aprobado en el anexo IV del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS).

CAPÍTULO II

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 4. Principios rectores y requisitos mínimos de seguridad.

Los principios básicos y requisitos mínimos de la seguridad de la información desarrollados bajo el marco de

esta Política de Seguridad de la Información (en adelante, PSI) son los recogidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en particular, los previstos en sus capítulos II y III, y en su normativa de desarrollo.

Artículo 5. Misión de la Administración de la Generalitat.

La Administración de la Generalitat se organiza y actúa dentro de su ámbito competencial con personalidad jurídica única, conforme a criterios de eficacia, publicidad, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al Derecho, dentro de la mayor economía de medios que permita la obtención de los fines que tiene encomendados en Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana, y en la Ley 5/1983, de 30 de diciembre, del Consell, conforme a la organización y atribuciones decretadas en cada momento por el president de la Generalitat.

Artículo 6. Marco regulatorio.

El marco normativo de las actividades de la PSI está integrado por todas las normas vigentes que afecten a la seguridad de la información en el ámbito de la Administración Electrónica de la Administración de la Generalitat.

Las acciones que la Administración de la Generalitat emprenda en materia de seguridad de la información serán acordes con las mejores prácticas de seguridad, recogidas en las guías del CCN-STIC del Centro Criptológico Nacional y otras normas internacionalmente reconocidas.

Artículo 7. Desarrollo normativo.

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará aplicando lo requisitos mínimos articulados en el capítulo III del ENS. Se estructurará en tres niveles, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente PSI.

b) Segundo nivel normativo: constituido principalmente por las normas y directrices de seguridad generales que, respetando lo estipulado por la PSI, determinan qué se puede hacer y qué no desde el punto de vista de la seguridad en relación con los servicios prestados por la Administración de la Generalitat, sin considerar aspectos relativos a implementación ni tecnológicos.

c) Tercer nivel normativo: constituido por políticas específicas que, respetando lo dispuesto en los niveles normativos anteriores, apliquen a ámbitos o sistemas de información particulares. También estará constituido por procedimientos, guías e instrucciones de carácter técnico o procedimental.

La documentación perteneciente a este tercer nivel normativo será aprobada por el Responsable del Sistema.

2. El Responsable del Sistema será el encargado de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma, para su ámbito de actuación.

3. El personal de cada uno de los órganos u organismos a los que es de aplicación la presente PSI tendrá la obligación de conocerla y cumplirla, tanto las normas como los procedimientos de seguridad de la información que puedan afectar a sus funciones.

Artículo 8. Riesgos derivados con el tratamiento de datos personales.

Para cada sistema de información, cuando trate datos personales, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizará un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, conforme al artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, una evaluación de impacto en la protección de datos.

En este caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el ENS, siendo el Responsable de Seguridad quien las integrará en un único plan de seguridad donde se contemplen todas las medidas técnicas y organizativas que deban implantarse.

CAPÍTULO III ORGANIZACIÓN DE LA SEGURIDAD

Artículo 9. Estructura, niveles de responsabilidad y roles de seguridad.

1. La organización de la seguridad de la información en cada entidad se estructura en tres niveles:
 - a) Nivel de gobierno:
 - i. La dirección de la entidad, quien ostenta la última responsabilidad, la coordinación entre los diferentes roles y la resolución de conflictos entre éstos.
 - ii. Los Responsables de la información.
 - iii. Los Responsables del servicio.
 - b) Nivel de supervisión:
 - i. El Responsable de Seguridad.
 - c) Nivel operativo:
 - i. El Responsable del Sistema.
 - ii. Los Administradores de Seguridad de Sistema.
2. La organización de la seguridad de la información de ámbito corporativo se articula en la CITEC.

Artículo 10. Los Responsables de la Información.

1. Será Responsable de la Información para cada sistema de información, a la persona titular del órgano superior o directivo, o en su caso del órgano colegiado, que ostente la competencia para determinar qué información trata.

2. El Responsable de la Información ejercerá en su ámbito de actuación las siguientes funciones:
 - a) Establecer los requisitos de la información en materia de seguridad, aprobando formalmente los niveles de seguridad de la información para cada dimensión de seguridad, dentro del marco establecido en el Anexo I del ENS; previa consulta al Responsable del Sistema e informando al Responsable de Seguridad.
 - b) Aprobar la asunción de los riesgos residuales que correspondan a la información.

Artículo 11. Los Responsables del Servicio.

1. Será Responsable del Servicio para cada sistema de información, a la persona titular del órgano superior o directivo, o en su caso del órgano colegiado, que ostente la competencia para determinar para cada sistema de información qué servicios presta.
2. El Responsable del Servicio ejercerá en su ámbito de actuación las siguientes funciones:
 - a) Establecer los requisitos del servicio en materia de seguridad, aprobando formalmente los niveles de seguridad del servicio para cada dimensión de seguridad, dentro del marco establecido en el Anexo I del ENS; previa consulta al Responsable del Sistema e informando al Responsable de Seguridad.
 - b) Aprobar la asunción de los riesgos residuales que correspondan a los servicios.

Artículo 12. El Responsable de Seguridad.

1. Será Responsable de Seguridad para todos los sistemas de información de la entidad, a la persona titular del órgano que tenga atribuidas las competencias sobre los servicios generales de la entidad.
2. Cada Responsable de Seguridad ejercerá en su ámbito de actuación las siguientes funciones:
 - a) Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
 - b) Supervisar la implantación y la eficacia de las medidas necesarias para garantizar que se satisfacen los requisitos.
 - c) Atender a la dirección de la entidad sobre todas las cuestiones de seguridad.
 - d) Realizar el análisis de riesgos y auditorías de seguridad junto al Responsable del Sistema, con la participación del Responsable de la información y Responsable del Servicio, acordando con dichos responsables las salvaguardas a implantar.
 - e) Promover la formación y la concienciación en materia de seguridad de la información.
 - f) Procurar la mejora continua del sistema de gestión de la seguridad de la información.
 - g) Realizar las actuaciones necesarias para el cumplimiento de las Instrucciones Técnicas de Seguridad.
3. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o números de usuarios se necesite de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, se podrán designar cuantos Responsables de Seguridad Delegados se consideren necesarios. Se designará como Responsables de Seguridad Delegados a empleados públicos,

que serán nombrados, por resolución administrativa, a propuesta del Responsable de Seguridad. La responsabilidad final sigue recayendo sobre el Responsable de Seguridad. Los delegados se harán cargo, en su ámbito, de todas aquellas funciones que le sean delegadas por el Responsable de la Seguridad. Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reporta. Estas delegaciones se realizarán conforme a los artículos 8, 9 y 12 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 13. Responsable del Sistema.

1. Será Responsable del Sistema para cada sistema de información, la persona titular del órgano directivo con competencias en materia de tecnologías de la información.
2. El Responsable del Sistema ejercerá en su ámbito de actuación las siguientes funciones:
 - a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
 - b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
 - c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
3. En determinados sistemas de información que, por su complejidad, distribución, separación física de sus elementos o números de usuarios se necesite de personal adicional para llevar a cabo las funciones del Responsable del Sistema, se podrán designar cuantos Responsable del Sistema Delegados se consideren necesarios. Se designará como Responsable del Sistema Delegados a empleados públicos, que serán nombrados, por resolución administrativa, a propuesta Responsable del Sistema. La responsabilidad final sigue recayendo sobre Responsable del Sistema. Los delegados se harán cargo, en su ámbito, de todas aquellas funciones que le sean delegadas por el Responsable del Sistema. Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reporta. Estas delegaciones se realizarán conforme a los artículos 8, 9 y 12 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 14. Administrador de la Seguridad del Sistema.

1. Será Administrador de la Seguridad del Sistema la persona titular de cada uno de los servicios en los que se organizan las unidades administrativas del órgano directivo con competencias en materia de tecnologías de la información.
2. El Administrador de la Seguridad del Sistema ejercerá en su ámbito de actuación las siguientes funciones:
 - a) Implementar, gestionar, mantener y monitorizar las medidas de seguridad en los sistemas de información.
 - b) Aplicar los procedimientos operativos de seguridad que apruebe el Responsable del Sistema.
 - c) Colaborar en la detección, investigación y resolución de incidentes de seguridad.

DISPOSICIONES ADICIONALES

Primera. Incidencia presupuestaria.

La aplicación y desarrollo de este decreto, no tendrá incidencia alguna en la dotación de todos y cada uno de los capítulos de gasto ya asignados en la Administración de la Generalitat.

Segunda. Inclusión al ámbito subjetivo de esta PSI.

Cualquier ente integrado en el sector público de la Generalitat, conforme al artículo 2 de la Ley 1/2015, de 6 de febrero, de Hacienda Pública, del Sector Público Instrumental y de Subvenciones, que guarde relación de vinculación, dependencia o adscripción con la Administración de la Generalitat, podrá quedar incluido en el ámbito subjetivo de esta PSI, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización del propio ente.

Tercera. Coordinación global de la ciberseguridad en la Administración de la Generalitat.

Conforme al Acuerdo del Consell sobre políticas de actuación en materia de ciberseguridad, aprobado en la reunión del día 23 de julio de 2021, la Dirección General de Tecnologías de la Información y las Comunicaciones asume la totalidad de la gestión de la ciberseguridad del Consell.

Cuarta. Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV).

CSIRT-CV es el centro de operaciones de ciberseguridad de la Administración de la Generalitat, prestador de servicios de prevención, detección y respuesta ante incidentes de ciberseguridad en el ámbito de la Administración de la Generalitat, de la ciudadanía, de las empresas y profesionales y del resto de las administraciones públicas de la Comunitat Valenciana.

La unidad administrativa que tenga atribuidas las competencias en ciberseguridad en la Dirección General de Tecnologías de la Información y las Comunicaciones, ejercerá la dirección del CSIRT-CV y el mando único en las operaciones de ciberseguridad para la gestión de crisis e incidentes de ciberseguridad, apoyará a los órganos directivos y a los órganos competentes en materia de seguridad, en las posibles situaciones de crisis de ciberseguridad que puedan tener impacto en la Comunitat Valenciana.

La Dirección General de Tecnologías de la Información y las Comunicaciones asume, en exclusiva para toda la Administración de la Generalitat, la totalidad de las actuaciones de coordinación con las autoridades competentes en materia de ciberseguridad nacional y con el resto de CSIRT de referencia nacionales e internacionales; incluidas las obligaciones de notificación obligatoria de los incidentes al Centro Criptológico

Nacional (CCN), la recopilación de evidencias y la remisión de estadísticas de incidentes, conforme a la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

DISPOSICIÓN DEROGATORIA

Única. Disposiciones que se derogan.

Quedan derogados:

1. El Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.
2. El Decreto 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat.
3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan o contradigan a lo dispuesto en el presente Decreto.

DISPOSICIONES FINALES

Primera. Ampliación de funciones de seguridad corporativa a la CITEC

Modificación del apartado 2 del artículo 3 del Decreto 112/2008, de 25 de julio, del Consell, por el que se crea la Comisión Interdepartamental para la Modernización Tecnológica, la Calidad y la Sociedad del Conocimiento en la Comunitat Valenciana, que queda redactado como sigue:

“Artículo 3. Naturaleza, competencias y funciones de la Comisión

1. (...)

2. En concreto, corresponde a la comisión CITEC:

a) Impulsar en el ámbito de cada departamento de la Administración de la Generalitat y de las entidades integrantes de su sector público dependiente, las políticas, programas, proyectos y actuaciones aprobados en ejecución de la planificación estratégica del Consell en las materias objeto de su competencia.

b) Ser informada preceptivamente de los planes, programas o líneas de actuación que se lleven a cabo por la Administración de la Generalitat o su sector público dependiente en relación con las materias objeto de su competencia.

c) Informar preceptivamente los anteproyectos normativos de la Administración de la Generalitat que se refieran o afecten a las materias objeto de su competencia.

d) Coordinar y realizar el seguimiento del nivel de implantación y desarrollo de las políticas de planificación, coordinación, autorización y control de las tecnologías de la información y las comunicaciones corporativas y la administración electrónica de la Administración de la Generalitat, de su sector público y de la Comunitat

Valenciana, y proponer iniciativas de mejora respecto de dichas materias y ámbitos.

e) Promover el intercambio de experiencias y la transferencia de conocimiento entre departamentos, organismos y entidades en relación con dichas materias.

f) Ofrecer soporte técnico al nivel operativo en las materias de su competencia y en los términos que se especifique por la propia comisión CITEC.

g) Cualesquiera otras funciones relacionadas con el ámbito de su competencia o que le sean atribuidas por la normativa vigente o por la que en el futuro se dicte, así como las que le encomiende el Consell por mandato específico o disposición de carácter general, y las que le deleguen los órganos con competencia en las materias señaladas.

h) Elaborar y revisar regularmente la política de seguridad de la información de la Administración de la Generalitat, para su aprobación por el Consell.

i) Aprobar las normas de seguridad pertenecientes a la documentación del segundo nivel normativo, conforme a la política de seguridad de la información de la Administración de la Generalitat.

j) Informar regularmente del estado de la seguridad de la información al Consell y atender sus inquietudes en esta materia, conforme a la política de seguridad de la información de la Administración de la Generalitat.

3. (..)".

Segunda. Organización de la seguridad en la Administración Sanitaria.

Se faculta a la persona titular de la conselleria con competencias en materia de sanidad y salud pública para que desarrolle las disposiciones necesarias para establecer la organización de la seguridad de la información en el ámbito de la Administración Sanitaria.

La organización de la seguridad tendrá en cuenta la organización propia de la Administración de la Generalitat. En consecuencia, deberá garantizarse la actuación coordinada y eficaz, según lo establecido al respecto en el ENS y en las orientaciones de la *Guía de Seguridad de las TIC CCN-STIC 801*, editada por el Centro Criptológico Nacional, sobre responsabilidades y funciones en el ENS.

Tercera. Organización de la seguridad en la Administración Educativa.

Se faculta a la persona titular de la conselleria con competencias en materia de educación para que desarrolle las disposiciones necesarias para establecer la organización de la seguridad de la información en el ámbito de la Administración Educativa.

La organización de la seguridad tendrá en cuenta la organización propia de la Administración de la Generalitat. En consecuencia, deberá garantizarse la actuación coordinada y eficaz, según lo establecido al respecto en el ENS y en las orientaciones de la *Guía de Seguridad de las TIC CCN-STIC 801*, editada por el Centro Criptológico Nacional, sobre responsabilidades y funciones en el ENS.

Cuarta. Organización de la seguridad en la Administración de Justicia.

Se faculta a la persona titular de la conselleria con competencias en materia de justicia para que desarrolle las disposiciones necesarias para establecer quien ha de ejercer, sobre los sistemas auxiliares de la Administración de Justicia en la Comunitat Valenciana, las funciones que sean determinadas por la Política de Seguridad de la Información Judicial Electrónica para las comunidades autónomas con competencias en justicia.

Quinta. Desarrollo.

Se faculta a la persona titular de la conselleria con competencias en materia de tecnologías de la información y comunicación para dictar cuantas disposiciones exija la aplicación y ejecución de este decreto.

Sexta. Entrada en vigor.

El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diari Oficial de la Generalitat Valenciana.